

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A SEARCH WARRANT**

I, Nicole S. Pinardo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Detective with the Beckley Police Department, Investigative Division. I have been so employed for approximately five years; however, I possess a combined total of approximately eleven years of experience as a law enforcement officer. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. I am a graduate of the West Virginia State Police Academy and hold an active law enforcement certification in the state of West Virginia. I am also currently deputized through the Department of Homeland Security and the West Virginia State Police as a Task Force Officer (TFO). I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18 U.S.C. §§ 2251, 2252 and 2252A.

3. As a Detective and TFO, I have investigated state and federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child

pornography that occur in the Southern District of West Virginia. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 (production of child pornography), 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

4. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat usernames that are stored at premises owned, maintained, controlled, or operated by Snap Inc. (“Snap”), a social networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snap to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B, related to Snapchat accounts for the username Jrod23014 (the “Subject Account”). Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography) and 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography) (the “Subject Offenses”) have been committed by Jarrod BENNETT. There is also probable cause to search the information described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

BACKGROUND ON SNAPCHAT¹

7. Snap, Inc. (“Snap”), the owner of Snapchat, is a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Snapchat is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Snapchat accounts like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Snapchat users.

8. Snap collects basic contact and personal identifying information from users during the Snapchat registration process. Snap also collects whether the account phone number has been verified.

9. Snap also collects and retains information about how each user accesses and uses Snapchat. This includes information about the Internet Protocol (“IP”) addresses used to create and use an account, unique identifiers and other information about devices and web browsers used

¹ The information in this section is based on information published by Snap on its website, including, but not limited to, the following document and webpages: “Snap Inc. Law Enforcement Guide,” available at <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf>; and “Snapchat Support,” available at <https://support.Snapchat.com/>.

to access an account, and session times and durations. Snap also collects account change history, which Snap describes as a log of changes in registration email or phone number, birthdate, and display name.

10. Each Snapchat account is identified by a username.

11. Snapchat offers four primary ways for users to communicate with each other.

a. **Snaps.** A user takes a photo or video using their camera phone in real-time. The user then selects a time limit of 1-10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone's photo gallery or just sent via Snapchat, without being saved. The photo/video can then be sent to a friend in Snapchat. The snap is deleted after the selected amount of time. If a recipient attempts to take a screenshot of the snap to save on his/her phone, the application will notify the sender of this behavior. Snapchat states that it deletes each snap from its servers once all recipients have viewed it. If a snap has not been viewed by all recipients, Snapchat states that it retains the snap for thirty days.

b. **Memories.** Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

c. **Stories.** A user can also add the photo/video Snap to their “Story.”

Depending on the user’s privacy settings, the photos and videos added to a Story can be viewed by either all users of Snapchat or just the user’s friends for up to 24 hours. Stories can also be saved in Memories.

d. **Chat.** A user can also type messages to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message (text or photo) that he or she wants to keep. The user can clear the message by tapping it again.

12. Snapchat also obtains a variety of non-content information from its users.

a. **Usage Information.** Snapchat may collect information about how users interact with its services, including which search queries they submit, and how they communicate with other users, including maintaining a log of all snaps to and from an account for the last 31 days, for 24 hours of posted Stories, and for any unopened Chats or those saved by a sender or recipient, and how a user interacts with these messages (such as when a user opens a message).

b. **Device Information.** Snapchat collects information about the devices of its users, including information about the user’s hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone; information from device

sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether the user has headphones connected; and information about the user's wireless and mobile network connections, such as mobile phone number, service provider, and signal strength. Snapchat can also provide the version of the application that is being used, the "last active" date the application was used, and whether two-factor-authentication is enabled.

c. **Device Phonebook.** Snapchat may collect information about the phonebook of the user's device.

d. **Cameras and Photos.** Snapchat may collect images and other information from the user's device's camera and photos.

e. **Location Information.** Snapchat may collect information about the user's location, including precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other device sensors, such as gyroscopes, accelerometers, and compasses.

f. **Snap Map.** Snapchat allows a user to share location information with his/her friends and also obtain location information about the user's friends. Based on such information, Snapchat places the friends' locations on a map viewable to the user. Snapchat can provide whether Snap Map was enabled.

g. **Information Collected by Cookies and Other Technologies.** Snapchat may collect information through cookies and other technologies about the user's activity, browser, and device.

h. **Log Information.** Snapchat collects log information when a user uses Snapchat's website, including device information, access times, pages viewed, IP address, and pages visited.

13. In my training and experience, evidence of who was using the above listed username and from where, and evidence related to the Subject Offenses, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

14. The stored communications and files connected to a Snapchat account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In fact, evidence is included in this affidavit detailing the use of Snapchat by BENNETT to commit the Subject Offenses.

15. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Snap can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier

information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

16. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

17. Therefore, Snap's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Snapchat. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

18. On or about April 18, 2023, Snapchat submitted CyberTip Report #157988246 to the National Center for Missing and Exploited Children ("NCMEC"). The incident type was identified as apparent child pornography, and the incident time was listed as: March 10, 2023, 19:29:24 UTC.

19. Snapchat uploaded one image file in connection with the report, which contained apparent child pornography. Snapchat reported that the file at issue was uploaded or shared by Snapchat username "thatoneguy26520." An email address of healer72@yahoo.com, and an IP address of 184.14.114.149 was provided by Snapchat for identification purposes. Snapchat viewed the entire contents of the uploaded file that was reported to contain child pornography.

20. On or about April 18, 2023, your Affiant reviewed the image file associated to the CyberTip and found it to contain a prepubescent male taking a photo of himself in the mirror while posing nude. This file was uploaded by Snapchat user “thatoneguy26520” on March 10, 2023.

21. On or about April 18, 2023, a state of West Virginia search warrant was obtained and served to Snapchat for all contact and personal identifying information, additional Snapchat accounts associated with the target account, all devices used and otherwise associated with the target account, all activity logs, all photos and videos uploaded by the account user, all profile information, all records of communications and messages made or received by the user, all check ins or any other location information, future and passed events the user responded to, all IP logs and associated port IDs, all records of the accounts usage of the like and follow features, all records of the accounts usage of the share feature, all information about the Snapchat pages that the account is or was a “fan” of, all records of Snap searches performed by the account, all information about the users access and use of marketplace, the types of services utilized by the user, all privacy settings and other accounts settings, and all records pertaining to the communications between Snapchat and any person regarding the user or the user’s Snapchat account associated with the Snapchat user “thatoneguy26520” between the dates of March 1, 2023 through April 16, 2023.

22. On or around May 24, 2023, your Affiant received a digital download of the requested account information from Snapchat for the username “thatoneguy26520.”

23. The information received showed the username of “thatoneguy26520” was created on February 20, 2023, and the account was disabled by Snapchat on March 10, 2023. During the 10-day span of information received, it shows the subject had sent approximately 9 different photos

and 8 different videos containing material depicting minors in sexually explicit conduct. The suspect had sent these files approximately 26 times to approximately 10 different people.

24. The photos sent included an image of young boys estimated to be approximately 7 years old standing nude, back-to-back, with erect penises and an image of what appears to be a toddler aged female's vagina being penetrated by an adult male's penis. The videos sent include several videos of prepubescent females masturbating and another video shows two young boys estimated to be around 8 years old nude. In the video one boy performs oral sex on the other boy.

25. Of note, a video from the "Memories" section of the Snapchat account showed what appeared to be a prepubescent female lying face down on a couch with a blanket covering her. The first video zooms in to focus on the child's buttocks. A second video shows a slender white male wearing only boxers stepping towards the child while stroking his exposed erect penis.

26. Further investigation revealed that the IP address provided in the Cybertip and Snapchat return resolved to Frontier Communications. The account listed a subscriber as Jarrod BENNETT with a service address of 115 Yaweh Ln Mount Nebo, WV 26679. At the time, BENNETT was employed as a deputy sheriff with the Nicholas County Sheriff's Department.

27. On June 5, 2023, a search warrant was obtained to search the Mount Nebo residence belonging to BENNETT. The search warrant was executed the same day. During the execution of the search warrant, several electronic devices were seized. It was also discovered the couch and surrounding area seen in the "Memories" video described in Paragraph 25 matched that seen in the BENNETT residence. It was later learned that an approximately 10-year-old female was residing with BENNETT at his residence.² Additionally, BENNETT's physical appearance is

² This minor female was later forensically interviewed and did not make any disclosures of abuse. However, this is not uncommon if a minor victim is asleep when an image or video is produced,

consistent with that of the slender white male depicted in the video described in Paragraph 25, and he is the only adult male residing in the home.

28. On June 21, 2023, I conducted a deconfliction search through the Internet Crimes Against Children (“ICAC”) Data System (“IDS”) using the email address of jrod14230@outlook.com, which law enforcement had previously identified as associated with BENNETT. The response from the search showed a NCMEC report number of 162944385, which had not yet been distributed to an agency.³ I requested the information from the tip and was sent a PDF of the tip by NCMEC.

29. The NCMEC Cybertip showed that Snapchat had reported username Jrod23014 for distributing a video file, which was confirmed by Snapchat to contain child pornography, on the date of May 29, 2023, at approximately 01:56:17 UTC.

30. In the Cybertip, Snapchat provided an email address of jrod14230@outlook.com as the email address used to create the account of Jrod23014. The account information also listed a date of birth that matched BENNETT’s date of birth.

31. On June 23, 2023, I viewed the reported video file and observed an adult male penetrating two prepubescent females’ vaginas with his penis. The girls are first seen on top of

and the minor in the video did not appear to be awake. Moreover, at the time of the forensic interview, the minor female and her mother still lived with BENNETT, a law enforcement officer, at his residence.

³ The Cybertip indicated that the IP address provided by Snapchat resolved back to Huntington, West Virginia, so the Cybertip would have been sent to the West Virginia ICAC after it was processed by NCMEC.

each other on their backs. After the penetration, the top child then moves to straddle the bottom child and they then begin to kiss each other.

CONCLUSION

32. Based on the foregoing, there is probable cause to believe that evidence related to the Subject Offenses may be located in the information described in attachment A.

33. Based on the foregoing, I request that the Court issue the proposed search warrant.

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Snap. Because the warrant will be served on Snap, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



Nicole S. Pinardo
Task Force Office
Department of Homeland Security
Homeland Security Investigations

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this

22nd day of December, 2023.



DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA